Binary Armor®
SCADA Network Data Guard

Cyber Security for Smart-Grid and Critical Infrastructure

Binary Armor® is an endpoint cyber security solution for SCADA and industrial control system networks. Designed to be installed in-line between PLCs, remote terminal units, intelligent electronic devices or controllers and the WAN/LAN, the Binary Armor® patented technology provides bi-directional security across all communication layers. Binary Armor® processes every byte of every message with a defined rule-set that is tailored to match the operational logic of the Industrial Control System on which it is deployed, ensuring only safe message traffic reaches critical systems. Binary Armor® cannot be modified or reconfigured without physical access to the system, providing a reliable and robust security solution to protect remote facilities and critical infrastructure.
Binary Armor®
SCADA Network Data Guard

Preventable Incidents at Industrial Control Systems

Binary Armor can prevent malicious HMI requests, blocks unauthorized commands and eliminates need for edge protection approach.

STUXNET
► Valve settings were modified

Night Dragon
► RAT and data exfiltration

Dragonfly
► Infected HMIs and data breach

SHAMOON
► Infected HMIs and data breach

Maroochy Shire
► The function of pumping station was modified

ICS Protocols and Security:
• DNP3, Modbus, EtherNet/IP, ROC Plus, HTTP, FTP, SMTP, NTP, Data-Diode, other custom protocols
• TLS 1.2 encryption with server and client verification for all protocols
• Out-of-the-box support for custom binary or ASCII protocols
• Key management through secure hardware token

Specifications
Size, Weight and Power:
• 5-32V VDC or 12-56 VDC
• 5.32” x 3.22” x 1.0”
• Weight: 1 lb
• Maximum power consumption: 5W
• Power and interface cable included

Interfaces:
• RS-232 or 3.3 V Digital IO on rugged power and data connector
• 10/100 Ethernet data interfaces on high and low side

Environmental:
• Operating temperature: -40° to +85° C
• Shock: 6g for 11ms
• Vibration: DO-160E CATS
• ESD: DO-160G Section 25
• Tamper-resistant enclosure